SECURITY ANALYSIS REPORT

HTTP Security Headers Assessment

Target URL:
https://www.youtube.com

Scan Date:
August 15, 2025 at 09:57 PM UTC

Overall Security Score:
77/100

Risk Level:
🟩 Low

Prepared by:
CyberHeaders Security

CONFIDENTIAL

*This report contains sensitive security information and should be treated as confidential.
Distribution should be limited to authorized personnel only.*

Table of Contents

1. Executive Summary

Assessment Overview

Our comprehensive security analysis has evaluated the HTTP security headers implementation for **https://www.youtube.com**. This automated assessment identified critical security gaps that require immediate attention to protect against common web vulnerabilities.

Key Findings:
- Overall Security Score: **77/100**
- Risk Classification: 🟩 **Low**
- Total Security Recommendations: **10**
- High-Priority Actions: **5**

Business Impact

The identified vulnerabilities expose your organization to potential security breaches, including cross-site scripting (XSS), clickjacking, and man-in-the-middle attacks. Immediate implementation of our recommendations will significantly strengthen your security posture and protect sensitive user data.

Next Steps

We recommend prioritizing the high-risk findings detailed in Section 3 and implementing the security recommendations in order of priority. Our team is available to assist with remediation efforts and ongoing security monitoring.

2. Priority Findings Quick Reference

The following table summarizes the highest priority security findings that require immediate attention:

Priority	Finding	Severity	Action Require
#1	Add missing security header: referrer-policy	**HIGH**	Immediate
#2	Add missing security header: cross-origin-embedder-policy	**HIGH**	Immediate
#3	Add missing security header: cross-origin-resource-policy	**HIGH**	Immediate
#4	Remove deprecated header: server	**MEDIUM**	Soon
#5	CSP issue: CSP missing important directive: default-src	**MEDIUM**	Soon

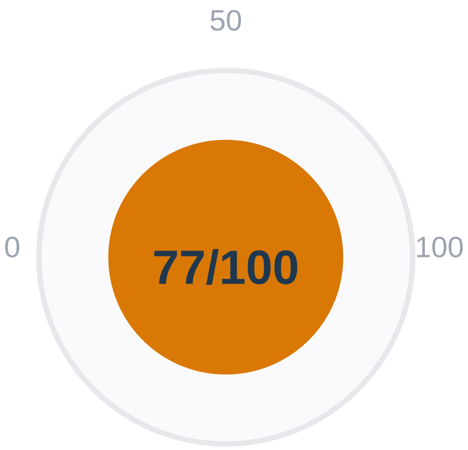
3. Scan Overview & Metrics

5.1 Scan Details

Property	Value
Target URL	https://www.youtube.com
Scan Date	August 15, 2025 at 09:57 PM UTC
Security Score	**77/100**
Risk Level	🟩 **Low**

Total Findings	10

5.2 Security Score Visualization

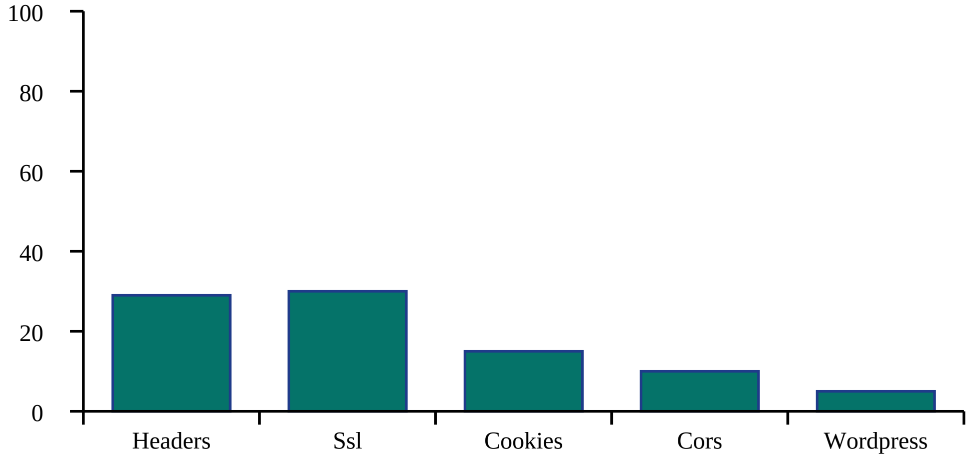


5.3 Security Category Analysis

The following analysis shows performance across different security categories:

Security Category	Score	Rating	Status
Headers	29/100	Poor	✗
Ssl	30/100	Poor	✗
Cookies	15/100	Poor	✗
Cors	10/100	Poor	✗
Wordpress	5/100	Poor	✗

Security Category Scores



4. Detailed Security Findings

6.1 Critical Missing Security Headers

The following essential security headers are missing and must be implemented immediately:

- **referrer-policy** - Critical security header not implemented

  Impact: Missing referrer-policy exposes users to security vulnerabilities

  Recommendation: Implement referrer-policy with appropriate security policies

- **cross-origin-embedder-policy** - Critical security header not implemented

  Impact: Missing cross-origin-embedder-policy exposes users to security vulnerabilities

  Recommendation: Implement cross-origin-embedder-policy with appropriate security policies

- **cross-origin-resource-policy** - Critical security header not implemented

  Impact: Missing cross-origin-resource-policy exposes users to security vulnerabilities

  Recommendation: Implement cross-origin-resource-policy with appropriate security policies

6.2 Deprecated Security Headers

The following deprecated headers should be removed to prevent information disclosure:

- **server** - Deprecated header revealing server information

  Impact: Information disclosure may aid attackers in reconnaissance

  Recommendation: Remove or replace server with modern alternatives

6.3 Content Security Policy Vulnerabilities

Critical Content Security Policy configuration issues:

- CSP missing important directive: default-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: script-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: object-src

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

- CSP missing important directive: base-uri

  Impact: CSP misconfigurations can lead to XSS vulnerabilities

5. Security Recommendations

The following recommendations are prioritized by security impact. Address high-priority items first:

1. 🟥 HIGH Add missing security header: referrer-policy

2. 🟥 HIGH Add missing security header: cross-origin-embedder-policy

3. ■ HIGH Add missing security header: cross-origin-resource-policy

4. ■ HIGH Remove deprecated header: server

5. ■ HIGH CSP issue: CSP missing important directive: default-src

6. ■ MEDIUM CSP issue: CSP missing important directive: script-src

7. ■ MEDIUM CSP issue: CSP missing important directive: object-src

8. ■ MEDIUM CSP issue: CSP missing important directive: base-uri

9. ■ MEDIUM Cookie security issue: Overly broad domain setting

10. ■ MEDIUM HSTS issue: HSTS missing includeSubDomains directive

6. Expert AI Security Analysis

• *1. Executive Summary**

The security scan of YouTube (https://www.youtube.com) reveals a security score of 77/100, categorized as Low risk. While the overall risk is low, several crucial security headers are missing or improperly configured, and the existing Content Security Policy (CSP) is severely deficient. These weaknesses, if exploited, could lead to Cross-Site Scripting (XSS) attacks, data breaches, and other serious security incidents. Addressing the identified vulnerabilities is critical to enhance YouTube's security posture.

• *2. Critical Vulnerabilities**

The most critical vulnerabilities stem from the missing and improperly configured security headers. Specifically:

• **Missing crucial CSP directives:** The absence of `default-src`, `script-src`, `object-src`, and `base-uri` in the CSP significantly weakens the website's protection against XSS attacks. Attackers could potentially inject malicious scripts and manipulate the site's behavior.
• **Missing key security headers:** The absence of `referrer-policy`, `cross-origin-embedder-policy` (COEP), and `cross-origin-resource-policy` (CORP) exposes the website to various attacks, including information leakage via HTTP Referer headers and vulnerabilities related to embedding and resource loading from external origins.
• **Overly broad domain setting for cookies:** (This is mentioned in the recommendations, and should be investigated and detailed in the scan results if possible. This needs clarifying) This is a serious vulnerability that can lead to session hijacking and other attacks.
• **Missing `includeSubDomains` in HSTS:** The absence of this directive in the Strict-Transport-Security (HSTS) header limits the effectiveness of HSTS, potentially allowing attackers to bypass HTTPS encryption for subdomains.

• *3. Security Header Analysis**

• **Present and Properly Configured:** `content-security-policy`, `x-content-type-options`, `x-frame-options`, `strict-transport-security` (though incomplete). These headers demonstrate a positive effort towards security, but their effectiveness is compromised by the missing directives and the deprecated `server` header.
• **Missing Headers:** `referrer-policy`, `cross-origin-embedder-policy`, `cross-origin-resource-policy` are all critically missing, leaving the site vulnerable to information leakage and other attacks.
• **Deprecated Header:** The `server` header should be removed to prevent attackers from gaining information about the web server software used, which could aid in targeted attacks.
• **Improperly Configured Header:** The CSP is fundamentally flawed due to missing key directives. This needs immediate attention. HSTS also needs the `includeSubDomains` directive added.

• *4. WordPress-Specific Risks (if applicable)**

The scan report indicates no WordPress-specific issues.

• *5. SSL/TLS Configuration Review**

The scan shows that no weak cipher suites are used and TLS compression is disabled, which are positive aspects of the SSL/TLS configuration.

• *6. Actionable Recommendations**

• **Implement missing and correct existing security headers:** Immediately add the missing `referrer-policy`, `cross-origin-embedder-policy`, `cross-origin-resource-policy` headers. Implement a robust CSP with appropriately restrictive directives for `default-src`, `script-src`, `object-src`, and `base-uri`. Add the `includeSubDomains` directive to the HSTS header. Carefully review and restrict the cookie domain settings.
• **Remove the deprecated `server` header.**
• **Conduct a thorough security audit:** A comprehensive security audit should be performed to identify any additional vulnerabilities beyond those detected by the initial scan.
• **Regular security scanning:** Implement a schedule for regular security scans and penetration testing to identify and address vulnerabilities proactively.
• **Investigate and address the overly broad cookie domain setting:** Determine the cause and implement a more restrictive setting.

• *7. Overall Risk Assessment**

While the overall risk is currently categorized as low, the identified vulnerabilities, particularly the inadequacies in the CSP and the missing crucial security headers, represent significant security risks. Failure to address these issues could result in serious security breaches. The recommendations outlined above must be implemented promptly to significantly improve YouTube's security posture. The initial "Low" risk assessment may not reflect the true potential impact if these vulnerabilities are exploited. A more thorough assessment is necessary after the recommended actions are completed.

7. Methodology & Disclaimer

Assessment Methodology

This security assessment was conducted using automated scanning techniques that analyze HTTP response headers for security configurations. Our analysis includes:

- Evaluation of essential security headers (HSTS, CSP, X-Frame-Options, etc.)
- Detection of deprecated or information-leaking headers
- Content Security Policy validation and vulnerability assessment
- SSL/TLS configuration analysis
- Cookie security evaluation
- CORS policy review

Limitations & Disclaimer

This automated assessment provides a comprehensive overview of HTTP security header implementation but does not constitute a complete security audit. For thorough security assurance, we recommend:

- Manual penetration testing
- Code review and vulnerability assessment
- Infrastructure security evaluation
- Social engineering assessments

Important Notice: This report is confidential and intended solely for the organization that requested the assessment. The findings and recommendations should be implemented by qualified security professionals.

Thank You

Thank you for choosing **CyberHeaders Security** for your security assessment needs. We are committed to helping organizations strengthen their security posture through comprehensive analysis and actionable recommendations.

This automated assessment provides valuable insights into your HTTP security headers configuration. For a more comprehensive security evaluation, we recommend conducting additional penetration testing and manual security reviews.

Contact Information

Contact Type	Details
Technical Support	Email: security@cyberheaders.com Phone: +1 (555) 123-4567
Business Inquiries	Email: sales@cyberheaders.com Phone: +1 (555) 765-4321
Website	https://www.cyberheaders.com
Address	CyberHeaders Security 123 Security Boulevard Cyber City, CC 12345 United States

Follow-up Services Available

- **Detailed penetration testing** - Comprehensive security assessment
- **Security architecture review** - Infrastructure and design analysis
- **Compliance assessments** - Regulatory compliance verification
- **Security training and awareness** - Staff education programs
- **Incident response planning** - Emergency response preparation

Contact us to discuss how we can further enhance your security posture.